CLAIMS

WE Claim:

1. A device for accessing information comprising an authentication system for verifying that the user of the device is the authorized user, the authentication system comprising:

a reader for sensing and reading a fingerprint of a user;

a memory for storing an authorized fingerprint;

a comparator, responsive to the reader and the memory, for comparing the read fingerprint to the stored fingerprint; and

a pseudo-random generator, responsive to the comparator, for generating a pseudo-random personal identification number (PIN) when the read fingerprint and the stored fingerprint are equivalent.

2. The device of claim 1, wherein said pseudo-random generator generates said PIN in accordance with a user specific algorithm.

3. The device of clam 2, further comprising a display for displaying said PIN, said PIN being forwarded by said user to an issuer of said device which grants access to said information.

4. The device of claim 3, wherein said issuer receives said PIN at an issuer network.

5. The device of claim 4, wherein said issuer network comprises:

a customer database having customer information for a plurality of users;

an issuer pseudo-random generator, responsive to said customer database, for generating a pseudo-random customer code, wherein said customer code is generated in accordance with said user specific algorithm; and

an issuer comparator, coupled to said customer database and said issuer generator, for comparing said customer code to said PIN, wherein the user is authorized and the device activation verified to access information when said customer code is equivalent to said PIN.

6. The device of claim 5, wherein said device a standard credit card being readable by a standard credit card reader.

7. The device of claim 5, wherein said device is a smart card.

8. The device of claim 5, wherein said device is a keyfob.

9. A method for verifying that a user of a device is an authorized user in order to access information, the method comprising the steps of:

sensing and reading a fingerprint of a user of the device;

comparing the read fingerprint with a stored fingerprint of the authorized user of the device; and

generating a pseudo-random personal identification number (PIN) when said read fingerprint is equivalent to the stored fingerprint, said PIN being used to verify activation of said device for accessing information.

10. The method of claim 9, wherein said PIN is generated in accordance with a user specific algorithm.

11. The method of claim 10, further comprising displaying said PIN to said authorized user on said device.

12. The method of claim 11, further comprising transmitting said PIN to an issuer of said device, wherein said issuer grants access to said information when said PIN is equivalent to a issuer generated code.

13. The method of claim 12, further comprising:

generating a pseudo-random customer code in response to the receipt by said issuer of said PIN;

comparing said customer code to said PIN;

verifying said user and activation of said device for accessing information when said customer code is equivalent to said PIN.

14. A system wherein an authorized user can access information through an access device issuer comprising:

an access device, including an authentication system for verifying that a user of the device is the authorized user, wherein the authentication system comprises:

a reader for sensing and reading a fingerprint of the user;

a memory for storing an authorized fingerprint;

a comparator, responsive to the reader and the memory, for comparing the read fingerprint to the stored authorized fingerprint; and

a pseudo-random generator, responsive to the comparator, for generating a pseudo-random personal identification number (PIN) in accordance with a user specific algorithm when the read fingerprint and the stored authorized fingerprint are equivalent, wherein the user uses the generated PIN to verify activation of the card for accessing information; and

an issuer network for receiving said PIN from said user, wherein the network comprises: a customer database having customer information for a plurality of users;

an issuer pseudo-random generator, responsive to said customer database, for generating a pseudo-random customer code, said customer code generated in accordance with said user specific algorithm; and

an issuer comparator, coupled to said customer database and said issuer generator, for comparing said customer code to said PIN, wherein said user and activation of said device for accessing information is verified when said customer code is equivalent to said PIN.